UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/492,632	01/27/2000	Ernst-Michael Hamann	GE998-005	1119

7590 07/07/2005

IBM Corporation
Anne Vachon Dougherty Esq
3173 Cedar Road
Yorktown, NY 10598

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/492,632	HAMANN ET AL.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 April 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11 and 13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11 and 13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This office action is in response to amendment filed on August 30, 2004. Original application contained Claims 1-15. Applicant previously cancelled claim 14, and amended Claims 1, 4, 5, 9, 11, and 12.

Applicant currently cancelled claims, 12, 15, and amended claims 1, 6, 9,11, and 13. The amendment filed have been entered and made of record.

2. Previous objection to drawings and specification and has been withdrawn.

3. Previous claim rejection under Claim Rejections under 35USC § 112, and § 101 and has been withdrawn.

4. Presently pending claims are 1-11, and 13.

Response to Arguments

Applicant's arguments filed on April 04, 2005 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1-11, and 13 applicants argued that " while cited prior art does receive R_3 as input information to the signature device, Applicant's believe that the cited prior art does not teach or suggest the steps and means for performing the steps of executing the signature program including the claimed creating and encrypting". Applicant also argued "that cited prior art does

mot teach or suggest the existence or use of an identifying characteristic of the hardware and software environment used for generating the digital signature".

This is not found persuasive. The system of cited prior art [Schaefer-Lorinser (U.S. Patent No. 6,662,151)] does teach a system and method for secure reading and processing of data on intelligent data media that uses code stored on IC cards in addition to data to be read and identification data, and provides code to master centre terminals for authentication of data media using symmetrical encoding technique

The system has a master centre with terminals having an interface suitable for temporary communications with the IC cards. A code stored on the cards in addition to the data to be read and identification data is available to the terminals for authentication of the data media according to a symmetrical encoding technique. Each card contains an individual code pair which satisfies the conditions for an asymmetrical code algorithm. The first code remains on the card as a signature function. The second code is passed to the reading terminal as a verification function for reading data media by testing the signature electronically transferred to the terminal (col.3 line 7 to col.4 line 52).

As a result, cited prior art does implement and teaches a system of signature devices and a method for generating digital signature as recited claims. Applicants still have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim

language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that cited prior art does teach or suggest the subject matter broadly recited in independent and subsequent dependent claims. Accordingly, rejections for Claims 1-11,and 13 are respectfully maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1-13, and 15 are rejected under 35 U.S.C. 102(e) as being anticipated by Schaefer-Lorinser (U.S. Patent No. 6,662,151 ("Schaefer-Lorinser " hereinafter).

2. With respect to claim 1, Schaefer-Lorinser teaches a method (Fig.2) for generating a digital signature in a signature device (i.e. chip card) having a signature program and certificate with signature key stored thereon and certificate with signature key stored thereon for the signing (col.3 line 52 to col.4 line 5) of a document (i.e. electronic purse), wherein the digital signature identifies at least one characteristic (i.e. device identification number) of the hardware and

software environment used for generating said digital signature in said signature device (col.3 line 56 to line 65, and Fig.2 Sglob attributes , and col.4 line 6 to line 13), comprising the step of:

receiving input information to said signature device (col.4 line 24 to line 26);

executing said signature program by the steps of: creating a signature data set comprising at least the received information, an identifier to identify said signature device device, at least one identifying characteristic of the hardware and software environment used for generating said digital signature (col.3 line 56 to line 65, and Fig.2 Sglob attributes), and a document extract value of the document for signing; and creating an expanded digital signature by encrypting (i.e. cryptogram e1) the signature data set with the aid of a signature key stored in said certificate (col.4 line 24 to line 51).

3. With respect to claim 9, Schaefer-Lorinser teaches an electronic signature device (i.e. chipcard) for generating a digital signature to sign a document (i.e. electronic purse) (Fig.2) comprising:

a receiver for receiving input information (Fig.1, and col.4 line 24 to line 26);

at least one storage location for storing (col.3 line 7 to line 10) at least a signature program and a certificate with signature key (col.3 line 52 to col.4 line 5);

a data processor component for executing said signature program comprising at least a component for creating a signature data set comprising at least the received information, an identifier to identify said signature device, at least one identifying characteristic (i.e. device identification number) of the hardware and software environment used for generating said digital signature col.3 line 56 to line 65, and Fig.2 Sglob attributes), and a document extract value of the

document (i.e. electronic purse) for signing (col.3line 10 to line 32); and an encryption component for creating an expanded digital signature by encrypting (i.e. cryptogram e1) the signature data set with the aid of a signature key stored at said signature device (col.4 line 24 to line 51).

4. With respect to claim 11, Schaefer-Lorinser teaches a method (Fig.2) a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine (Fig.1, computer center, and chipcard) to perform method steps for generating a digital signature to sign a document in a signature device having a signature program and certificate with signature key stored thereon (col.3 line 52 to col.4 line 5), said method steps comprising:

receiving input information to said information device (Fig.1, and col.4 line 24 to line 26);

executing said signature program by the steps of creating a signature data set comprising at least the received information, an identifier to identify said signature device, at least one identifying characteristic (i.e. device identification number) of the hardware and software environment used for generating said digital signature (col.3 line 56 to line 65, and Fig.2 Sglob attributes), and a document extract value of the document for signing (col.3 line 10 to line 32); and creating an expanded digital signature by encrypting (i.e. cryptogram e1) the signature data set with the aid of a signature key stored in said certificate (col.4 line 24 to line 51).

6. Claims 2, 4-6, 10, and 13are rejected applied as above in rejecting Claims 1, 9, and 12. Furthermore, Schaefer-Lorinser teaches a system that relates to digital signatures, methods for generating digital signatures, and signature devices to execute the methods.

As per claim 2, wherein said receiving input information (i.e. identification number) comprises procuring the value of a signature counter from said signature device (col.4 line 17 to line 23).

As per claim 4, wherein the receiving input information comprises procuring the identifying characteristic to identify the signature device from said signature device (col.4 line 36 to line 51).

As per claim 5, wherein the receiving input information comprises procuring information as to the hardware and software environment used in creating the digital signature (col.3 line 23 to line 32).

As per claim 6, further comprising entering an identifying characteristic to identify a holder of the signature key prior to said receiving input information (col.4 line 23 to line 45).

As per claim 10, wherein the device is a chipcard.

As per claim 13, wherein said at least one identifying characteristic comprises information which uniquely identifies said digital signature in relation to every other digital signature generated with the same signature key (col.4line 45 to line 51).

7. Claims 3, 7, and 8 are rejected applied as above in rejecting Claims 2, and 6. Furthermore, Schaefer-Lorinser teaches a system that relates to digital signatures, methods for generating digital signatures, and signature devices to execute the methods.

As per claim 3, further comprising, prior to said procuring, creating the signature counter as an attribute of the signature key (i.e. signature function Scard, stored attribute of this function, such as money, and chipcard posting/sequence number record stored in chipcard) (col. 4 line 23 to line 65).

As per claim 7, further comprising creating the identifying characteristic to identify the holder of the signature key as an attribute of the signature key (col.4 line 23 to line 45).

As per claim 8, further comprising changing the identifying characteristic to identify the holder of the signature key prior to said receiving (col.4 line 23 to line 45).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

sz
June 26, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100